Book Reviews

Breaking Security Design Bottlenecks in Payment Technologies

Godfried Williams • University of East London

Payment Technologies for E-Commerce
Weidong Kou, ed.
344 pages
US$69.95
Springer, 2006
ISBN: 3-540-44007-0

The subject of payment technology is central to e-business applications. Payment technologies’ main role is to facilitate transactions by saving time and providing cost effectiveness, value for money, and flexibility for consumers. Payment Technologies for E-Commerce provides brings to light electronic payment systems that serve as the backbone for payments made electronically. The book also emphasizes the strategic importance and shortfalls during implementation of such systems. It highlights advances that are likely to rectify the technological problems associated when adopted in business.

In the introduction, Weidong Kou scopes the book’s essential topics by examining credit cards’ role in e-business transactions and the Internet’s role in payment technologies. He also discusses the importance of security standards and protocols, including SSL (secure sockets layer), SET (secure electronic transaction), and IPsec (IP security). These technologies are central to secure, successful credit card payments. The introduction heavily emphasizes mobile payments and wireless systems because they’re hot topics in academia and industry. The introduction also emphasizes the role of software agents, which perform useful services on behalf of customers who surf the Internet or search for generic services.

Although the introduction discusses payment technologies and security methods, it doesn’t highlight areas related to vulnerability assessment. This is important to readers and clients who use payment technologies because they’re often naïve about the information being protected (in other words, they’re not fully aware of their vulnerability).

Security and authentication

In chapter 2, Fangguo Zhang and Yumin Wang discuss security issues and common algorithms applied in e-business. This level of detail is relevant for understanding the issues associated with ensuring confidentiality and data integrity. Zhang and Wang also discuss encryption and crypto-systems, providing useful insights to newcomers and experienced enthusiasts alike. They explore authentication in a way that will enlighten both technical and nontechnical readers. They place some importance on server-side security and elaborate on confidentiality, integrity, availability, nonrepudiation, authentication, auditing, and third-party systems as requirements for facilitating e-business transactions. The chapter also throws light on issues related to trust, access control, and corporate security. It’s comprehensive enough to whet the appetite of any enthusiastic graduate or undergraduate, or anyone else interested in cryptography’s underlying concepts.

Zhang and Wang also emphasize the power of quantum computing and practical issues associated with its use and application. This research area is related to polynomials and discrete logarithms and
could well be exploited by students interested in mathematics. The authors similarly assess DNA computing, highlighting its limitations in the real world. The chapter also examines hash functions, such as SHA-1 and MD5, and random-number generators.

In chapter 3, Hui Li and Wang present public-key infrastructure and related challenges by examining systems for publishing public-key cryptographs. PKI combines software, encryption technologies, and services to prevent confidentiality breaches, enabling enterprises to protect communication infrastructure and business forecasting. PKI uses a holistic approach, integrating digital certificates, public key cryptographs, certification, and an enterprise wide-area network architecture. Problems associated with certification authorities and bodies, however, sometimes shake PKI’s foundations, and PKI also raises issues related to trust, law, and existing regulatory frameworks.

This chapter also comprehensively assesses the roles of certification, design, and issuing methods among enterprises. Li and Wang elaborate on several commonly available and widely used certification schemes. A synergy exists between certification, standards, and the third parties that issue them. Although the authors express a concise view of these certificates’ role, they don’t explore associated problems (such as trust issues). A detailed discussion of such issues would enable the research community to assess possible solutions. On the whole, however, the information in the chapter is important and timely.

David Zhang and Li Yu discuss biometrics’ role and security applications in chapter 4. Although evidence suggests that people are becoming more interested in biometrics, many in industry and the research community are skeptical about its effectiveness. Zhang and Yu present a scholarly exposition of the topic, including vivid pictorial representations of the physical features captured for deploying biometric security systems. Although they assert that biometrics provides the most secure systems, this is debatable. The chapter describes and examines the attributes of finger, hand, retina, iris, facial, signature, and voice scans; facial and hand geometry; dynamic signature verification; and speaker verification. A useful template and system chart illustrates how such systems work, helping researchers and enthusiasts understand a biometric system’s dynamics. The technology could be applied in areas such as physical-access control (for example, to buildings) and for authenticating e-learning systems. Fingerprinting is seen as a means of improving online banking transactions and fraud protection and as a way to boost customer confidence. The chapter’s detailed overview of biometric systems and methods would be highly useful for undergraduates, graduates, academics, and practitioners interested in biometric security.

Smart cards, wireless infrastructure, and payment agents

Weidong Kou, Simpson Poon, and Edwin M. Knorr present smart card applications in chapter five. They begin by describing smart cards’ genesis in 1974, along with their make-up and architectural constitution. They describe different types of smart cards and present an architectural overview of the technology. They also mention the TCP/IP reference model and its relationship with smart card readers. They also discuss Java and Octopus smart cards, which have many applications in the travel industry, communication, and personal security.

This chapter is a useful foundation for smart card technology devotees. Statistical data provides insights for smart card technology users worldwide. Electrical engineering students pursuing artificial intelligence could explore architectural constraints and optimization techniques.

In chapter six, Kou dissects wireless-technology infrastructure, although not in great detail. He does, however, provide useful, relevant information on the communication systems that support the infrastructure. He also elaborates on the applications that wireless systems support and introduces wireless transport layer security, the wireless datagram protocol, and the wireless application protocol gateway. He presents the WAP model using illustrations depicting the WAP gateway’s role in communication. For readers and researchers interested in the scripting languages driving these systems, this chapter provides simple, concise examples.
In chapter seven, Amitabha Das examines payment agents, software agents that make payments on clients’ behalf. The chapter serves as an excellent foundation for developers wanting to develop mobile applications with intelligent capabilities and functions. Das differentiates between agents that facilitate transactions and mobile agents that migrate autonomously between computer networks. He also highlights the main phases (withdrawal, distribution, payment, verification, and transfer) of a secured payment protocol for agents and includes a well-explained set of notations.

Digital cash and checks
Chapter eight highlights three types of digital cash schemes: digital cash, fair digital, and Brand’s digital cash. Yi Mu, Vijay Varadharajan, and Khanh Quoc Nguyen explore concerns that law enforcement agencies will likely raise about these systems and the accompanying policies for processing transactions. They believe that large deployments of digital cash and checks will be difficult to manage and could be vulnerable to criminal activity. The authors also outline security requirements for digital cash, which is useful information for any security manager or auditor. This chapter throws lots of challenges to security auditors and researchers interested in information systems auditing. It would be appropriate for developers wanting to explore different digital schemes, design concepts, and associated protocols, and for final-year undergraduates and graduate students.

In chapter nine, about digital checks, Bo Yang emphasizes authentication processes and explains encryption methods. He also clearly outlines the phases of applying digital checks.

Secure transactions
Chapters 10, by Gordon Agnew, and 11, by Johnny Wong, Lev Mirlas, Kou, and Xiaodong Lin, present concepts and issues affecting secure transactions and throw light on application-layer security. The bedrock of chapter 10 is SET (Secure Electronic Transaction), a standard drawn from contributions from VISA and MasterCard that relies more on digital certificates than conventional methods, which mainly rely on trust. Although highly robust, SET has performance-related problems and lacks mutual authentication capabilities.

Agnew also discusses two other security protocols deployed as part of the TCP/IP protocol suite—IPsec and SSL—and examines the implications of layered security (a feature of IPsec). Although SSL has its strengths, recent developments have revealed key vulnerabilities. Chapter 11 outlines the steps in implementing a credit card-based secure online payment scheme. It also highlights trust problems linked with online payments.

In chapter 12, Amir Herzberg discusses the practicalities and challenges of micropayment systems. The assessment provides a conceptual view and highlights issues that must be conquered for micropayment systems to function effectively. Although Herzberg gives an overview of the payment service provider micropayment model, detailed discussions of different models would have been useful.

Herzberg also discusses the major categories of cost. This information is essential for practitioners who intend to develop or investigate models critical in assessing the cost of disputes, refunds, customer support, and so on. This chapter provides a general, broad overview for researchers wanting to learn about the rules and laws that protect consumer interests and ensure that merchants and service providers meet their obligations throughout the transaction. Herzberg also discusses servers that support micropayment systems. For distributed systems engineers, this is something to explore.

Final remarks
Chapters 13, by Zheng Huang, Dong Zheng, Zichen Li, and Kou, and 14, by Kou, draw conclusions from the rest of the book. They review industrial e-payment systems and solutions and assess opportunities for students, developers, and researchers. The discussions of the design, goals, and functions of industrial payment mechanisms are useful. The dialogue is based on a few particular systems, including VISA Cash, iPIN, and PayPal. The authors also give an architectural overview of
these systems. Chapter 13 provides an excellent summary of the fundamentals of payment solution systems. Data flows and structure charts aid Kou’s explanations. This chapter also discusses the technology supporting PayPal.

*Payment Technologies for E-Commerce* is a comprehensive book that broadly covers technologies essential for facilitating electronic transactions. The topics it presents are timely. Future editions of the book could consider standards and policies associated with e-payment systems, including quality and security standards in both advanced and developing economies; the current edition seems to apply mostly to advanced economies. Other possible topics to cover include design requirements of e-payment systems, as well as related social, legal, and ethical issues.

**Godfried Williams** is a senior lecturer at the University of East London. Contact him at g.williams@uel.ac.uk.

**Related Links**

- DS Online's Security Community
- "Cybercrimes against Consumers: Could Biometric Technology Be the Solution?" *IEEE Internet Computing*

**Cite this article:**